University of Colombo, Sri Lanka

University of Colombo School of Computing

DEGREE OF BACHELOR OF INFORMATION TECHNOLOGY (EXTERNAL)

Academic Year 2024 — 3rd Year Examination — Semester 6

IT6406 — Network Security and Audit

Structured Question Paper
(2 Hours)

To be completed by the candidate

Index Number							

Important Instructions

- The duration of the paper is **2 hours**.
- The medium of instructions and questions is English. Students should answer in the medium of English language only.
- This paper has **4 questions** on **10 pages**. Answer **all** questions.
- All questions carry **equal** marks.
- Write your answers **only on the space provided** on this question paper.
- Do not tear off any part of this question paper. Under no circumstances may this paper (or any part of this paper), used or unused, be removed from the Examination Hall by a candidate.
- Note that questions appear on both sides of the paper. If a page or part of a page is not printed, please inform the supervisor/invigilator immediately.
- Any electronic device capable of storing and retrieving text, including electronic dictionaries, smartwatches, and mobile phones, is not allowed.
- Calculators are **NOT allowed**.
-

To be completed by the examiners

1	
2	
3	
4	
Total	

Index Number | | | | | | | |

1. (a). Describe the primary motivation for implementing a firewall within an organisational network infrastructure.

[5 marks]

(b). Firewalls employ various techniques to regulate network access. Given that service control is one such method, list down three (3) other distinct techniques used by firewalls for access control.

[3 marks]

(c). Explain the mechanism by which firewalls implement access control using the service control technique.

[5 marks]

Index Number | | | | | | | |

(d). Identify and briefly list four (4) distinct types of firewalls commonly employed in network security.

[4 marks]

(e). Provide a detailed illustration, in the form of a diagram, outlining the DomainKeys Identified Mail (DKIM) signing and verification process. The diagram should clearly depict all essential components involved in this email authentication mechanism and their interactions.

[8 marks]

Index Number | | | | | | | |

2. (a). Describe the characteristics of an ad hoc network and explain the primary security challenges inherent in such network configurations.

[4 marks]

(b). Write down three (3) methods of securing wireless networks.

[6 marks]

Index Number | | | | | | | |

(c). Explain the inherent security risks associated with utilising untrusted network environments.

[6 marks]

(d). Maintaining compliance requires a well-defined, systematic approach that integrates both processes and technology. Briefly describe two (02) essential components that should be included in the approach to maintain compliance.

[5 marks]

(e). List down four (4) components of a typical IT infrastructure.

[4 marks]

3. (a). Transport Layer Security (TLS) is a combination of protocols working together to secure information communication.

i. What is the Phase III of Handshake Protocol in TLS?

[2 marks]

ii. Explain the main steps of the Phase III of TLS protocol.

[6 marks]

(b). Describe the steps involved in a replay attack on an information system and explain two (2) methods that you can use to prevent or reduce the possibility of such attacks.

[8 marks]

(c). Describe Federated Identity using an example.

[5 marks]

Index Number | | | | | | | |

(d). A framework offers IT organizations a method for establishing an approach to managing IT risks. COBIT5 is such a framework. Write the five COBIT5 principles.

[4 marks]

4. (a). Use a diagram to explain the flow of processing a packet in the network layer of IP Security implementation.

[8 marks]

Index Number | | | | | | | |

(b). In IP Security, what is the purpose of Security Parameter Index (SPI)?

[3 marks]

(c). Describe the technique used by Kerberos protocol for distributing the session keys.

[8 marks]

Index Number | | | | | | |

(d). List down and briefly describe four (04) deployment models of cloud computing.

[6 marks]

****